IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: Harrison, *et al.*	)	Confirmation No: 2570
	)	Group Art Unit: 2137
Serial No.: 09/918,062	)	
	)	Examiner: Davis, Zachary A.
Filed: July 30, 2001	)	
	)	Atty. Docket No.: 30006786-2
For: Authenticating Facsimile Documents Using Digital Signatures	)	

AMENDED APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Amended Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed August 23, 2007, responding to the final Office Action mailed May 24, 2007.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC, headquartered in Palo Alto, CA.

II. Related Appeals and Interferences

A related application having serial number 09/918,326 is currently pending with the Board of Patent Appeals.

III. Status of Claims

Claims 1-19 stand finally rejected. No claims have been allowed. The rejections of claims 1-19 are appealed.

IV. Status of Amendments

No amendments have been made subsequent to the final Office Action mailed May 24, 2007. An account of the claim amendments that have been made in the present application is provided hereafter.

This application was originally filed on July 30, 2001, with nineteen (19) claims. In a Response filed May 12, 2005, Applicant amended claims 1, 3, 5, 9, 11, and 14-19. In a Response filed November 30, 2005, Applicant amended claims 1, 5, 9, 18, and 19. In a Response filed May 16, 2006, Applicant amended claims 1, 3, 9, 18, and 19. In a Response filed October 24, 2006, Applicant presented remarks without any claim amendments. In a Response filed March 8, 2007, Applicant amended claims 1 and 14. The claims in the attached Claims Appendix (see below) reflect the present state of Applicant's claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a method of delivering and determining the authenticity of a digital document (Figure 1, 24) sent by an unknown sender to an intended recipient at a printout station (Figure 1, 16). The method comprises receiving and securely retaining a digital document (Figure 1, 24), a transmitted independently verifiable data record (Figure 1, 18) of the intended recipient at a printout station (Figure 1, 16), and an encrypted digest (Figure 4, 86) of the document created by the sender using a

hash algorithm (Figure 4, 84). Applicant's specification, page 16, lines 21-26; page 22, lines 17-22; and page 23, lines 26-28. The digest (Figure 4, 86) is encrypted using a first token (Figure 4, 26) of the sender. Applicant's specification, page 24, lines 2-3. The method further comprises obtaining a second token (Figure 4, 20) of the sender relating to the first token (Figure 4, 26) of the sender and obtaining a first token (Figure 4, 20) of the intended recipient. The method also comprises decoding the encrypted digest (Figure 4, 86) using the second token (Figure 4, 20) of the sender, using a hash algorithm (Figure 4, 92) to create a digest of the document, and comparing the decrypted received digest (Figure 4, 86) with the newly created digest to determine the authenticity of the sender and the document (Figure 1, 24). Applicant's specification, page 24, lines 15-21. The method further comprises requesting proof of the intended recipient's identity at the printout station (Figure 1, 16) using data in the independently verifiable data record (Figure 1, 18) of the intended recipient and decoding encrypted identification data (see Applicant's specification, page 25, lines 15-21) with the first token (Figure 4, 26) of the intended recipient. Applicant's specification, page 16, lines 14-20. The encrypted identification data (see Applicant's specification, page 25, lines 15-21) is identification data from the independently verifiable data record (Figure 1, 18) that is encrypted using a second token (Figure 4, 20) of the recipient by a transmitting station (Figure 4, 72). Applicant's specification, page 25, lines 15-21. Such a method also comprises comparing the decrypted identification data (see Applicant's specification, page 25, lines 15-21) with contents of the independently verifiable

data record (Figure 1, 18) to determine the authenticity of the recipient of the document (Figure 1, 24) and releasing the document (Figure 1, 24) when the intended recipient has proved their identity by use of the first token (Figure 4, 26) of the intended recipient that is uniquely related to the second token (Figure 4, 20) of the intended recipient. Applicant's specification, page 16, lines 14-20; page 17, lines 6-8; and page 29, lines 8-21.

Embodiments according to independent claim 9 describe a method of sending and delivering a digital document (Figure 1, 24) to an intended recipient at a printout station (Figure 1, 16) together with data enabling the document (Figure 1, 24) and the sender to be authenticated. The method comprises creating a digest (Figure 4, 86) of the document (Figure 1, 24) using a hash algorithm (Figure 4, 84), obtaining a first token (Figure 4, 20) of the intended recipient, and encrypting the digest (Figure 4, 86) using a first token (Figure 1, 26) of the sender. Applicant's specification, page 16, lines 21-26; page 22, lines 17-22; and page 23, lines 26-28. The method further comprises obtaining a second token (Figure 4, 20) of the sender relating to the first token (Figure 4, 26) of the sender, which can be used to decrypt the encrypted digest (Figure 4, 86), encoding identification data (see Applicant's specification, page 25, lines 15-21) of the intended recipient using the first token (Figure 4, 20) of the intended recipient, and sending the encrypted digest (Figure 4, 86), the digital document (Figure 4, 24), the second token (Figure 4, 20) of the sender, and the encoded identification data (see Applicant's specification, page 25, lines 15-21) to the recipient. Applicant's specification, page 21, lines 11-15 and pages 23-24, lines

24-12. Such a method also comprises receiving and securely retaining a transmitted document (Figure 1, 24), the encoded identification data (see Applicant's specification, page 25, lines 15-21), and a transmitted independently verifiable data record (Figure 1, 18) of the intended recipient at a printout station (Figure 1, 16); requesting proof of the intended recipient's identity at the printout station (Figure 1, 16) using data in the independently verifiable data record (Figure 1, 18) of the intended recipient; and decoding the identification data (see Applicant's specification, page 25, lines 15-21) of the intended recipient using a second token (Figure 4, 26) of the intended recipient. Applicant's specification, page 16, lines 14-20. The method further comprises comparing the decoded identification data (see Applicant's specification, page 25, lines 15-21) with contents of the independently verifiable data record (Figure 1, 18) to determine the authenticity of the recipient of the document (Figure 1, 24) and releasing the document (Figure 1, 24) when the intended recipient has proved their identity by use of the second token (Figure 4, 26) of the intended recipient that is uniquely related to the first token (Figure 4, 20) of the intended recipient. Applicant's specification, page 16, lines 14-20; page 17, lines 6-8; and page 29, lines 8-21.

Embodiments according to independent claim 18 describe a device for delivering and determining the authenticity of a digital document (Figure 1, 24) sent by an unknown sender to an intended recipient at a printout station (Figure 1, 16). The device comprises a communications module (see Applicant's specification, page 29, lines 22-26) arranged to receive an electronic version of the transmitted document (Figure 1, 24) over a communications network (Figure

7, 158), an independently verifiable data record (Figure 1, 18) of the intended recipient, a first token (Figure 4, 20) of the intended recipient, an encrypted digest (Figure 4, 86) of the document (Figure 1, 24) created by the sender using a hash algorithm (Figure 4, 84), a second token (Figure 4, 20) relating to a first token (Figure 4, 26) of the sender, and encrypted identification data (see Applicant's specification, page 25, lines 15-21) of the intended recipient. The digest (Figure 4, 86) is encrypted using the first token (Figure 4, 26) of the sender. Applicant's specification, page 16, lines 21-26; page 22, lines 17-22; and page 23, lines 26-28. The encrypted identification data (see Applicant's specification, page 25, lines 15-21) is encrypted using a first token (Figure 4, 20) of the intended recipient. Applicant's specification, page 25, lines 15-21 The device further comprises a store (Figure 4, 88) for securely retaining the transmitted document (Figure 1, 24), the transmitted independently verifiable data record (Figure 1, 18) and the first token (Figure 4, 20) of the intended recipient; and an instruction module (see Applicant's specification, page 6, lines 8-10) for requesting proof of the intended recipient's identity using data provided in the intended recipient's data record (Figure 1, 18). Applicant's specification, page 16, lines 14-20. Such a device also comprises a controller (see Applicant's specification, page 9, lines 5-6) arranged to decode the encrypted digest (Figure 4, 86) using the second token (Figure 4, 20) of the sender, Applicant's specification, page 9, lines 5-6; create a digest of the document using a hash algorithm (Figure 4, 92), Applicant's specification, page 9, lines 9-15; compare the decrypted received digest with the newly created digest to determine the

authenticity of the sender and the document (Figure 1, 24), Applicant's specification, page 9, lines 7-8; and release the document (Figure 1, 24) when the intended recipient has proved their identity by use of a second token (Figure 4, 26) of the intended recipient that is uniquely related to the first token (Figure 4, 20) of the intended recipient. Applicant's specification, page 8, lines 10-12. The second token (Figure 4, 26) of the intended recipient is used to decode encrypted identification data (see Applicant's specification, page 25, lines 15-21) of the intended recipient that is compared to contents of the independently verifiable data record (Figure 1, 18) of the intended recipient to determine authenticity of the intended recipient. Applicant's specification, page 16, lines 14-20; page 17, lines 6-8; and page 29, lines 8-21.

Embodiments according to independent claim 19 describe a device for sending and delivering a digital document (Figure 1, 24) to an intended recipient at a printout station (Figure 1, 16) together with data enabling the document (Figure 1, 24) and the sender to be authenticated. The device comprises a controller (see Applicant's specification, page 9, lines 11-12) arranged to create a digest (Figure 4, 86) of the document (Figure 1, 24) using a hash algorithm (Figure 4, 84) and to encrypt the digest (Figure 4, 86) using a first token (Figure 4, 26) of the sender and to encrypt identification data (see Applicant's specification, page 25, lines 15-21) of the intended recipient using a first token (Figure 4, 20) of the intended recipient. Applicant's specification, page 16, lines 21-26; page 22, lines 17-22; and page 23, lines 26-28. The device further comprises a communications module (see Applicant's specification, page 9, lines

12-15) arranged to obtain a second token (Figure 4, 20) of the sender related to the first token (Figure 4, 26) of the sender, which can be used to decrypt the encrypted digest (Figure 4, 86) and to send the encrypted digest (Figure 4, 86), the digital document (Figure 4, 24), the second token (Figure 4, 20) of the sender, the encrypted identification data (see Applicant's specification, page 9, lines 11-12) of the intended recipient, and the first token (Figure 4, 20) of the intended recipient to the recipient. Applicant's specification, page 21, lines 11-15 and pages 23-24, lines 24-12.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1-12 and 14-19 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Linsker* (U.S. Patent No. 5,598,473) in view of *Mazzagatte* (U.S. Patent No. 6,862,583) in further view of *Davis* (U.S. Patent No. 5,633,932) in further view of *Menezes* (Handbook of Applied Cryptography).

Claim 13 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* in further view of *Clark* (U.S. Patent 5,448,045).

VII. Arguments

The Appellant respectfully submits that Applicant's claims 1-19 are patentable. The Appellant respectfully requests that the Board of Patent Appeals overturn the rejection of those claims at least for the reasons discussed below.

A. The *Linsker* Reference

Linsker describes an authentication method that verifies if a received document comes from a purported sender and has not been altered during transmission. *See* cols. 1-2, lines 66-2. *Linsker* does not disclose that information is encrypted using a token of an intended recipient and then transmitted. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

B. The *Mazzagatte* Reference

Mazzagatte describes that print data received by a print node is encrypted at the print node and stored until the print node receives authentication from an intended recipient. *See* col. 2, lines 13-20. Accordingly, *Mazzagatte* discloses that encryption and decryption operations are both performed at a print node. Further, *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes.

C. The *Davis* Reference

Davis describes a system where a sending node encrypts a document using a public key of a printing node, where the printing node will use its private key to decrypt the document after it is received by the printing node. As such, *Davis* discloses that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. This header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

D. The *Menezes* Reference

Menezes refers to the Handbook of Applied Cryptography. *Menezes* does not disclose using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient.

E. Applicant's Claims 1-12 and 14-19

Claims 1-12 and 14-19 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Linsker* (U.S. Patent No. 5,598,473) in view of *Mazzagatte* (U.S. Patent No. 6,862,583) in further view of *Davis* (U.S. Patent No. 5,633,932) in further view of *Menezes* (Handbook of Applied Cryptography).

1. Claim 1

As provided in independent claim 1, Applicant claims:

A method of delivering and determining the authenticity of a digital document sent by an unknown sender to an intended recipient at a printout station, the method comprising:

receiving and securely retaining a digital document and a transmitted independently verifiable data record of the intended recipient at a printout station, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender;

obtaining a second token of the sender relating to the first token of the sender;

obtaining a first token of the intended recipient;

decoding the encrypted digest using the second token of the sender;

using a hash algorithm to create a digest of the document;

comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document;

requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient;

decoding encrypted identification data with the first token of the intended recipient, the encrypted identification data being identification data from the independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station;

comparing the decrypted identification data with contents of the independently verifiable data record to determine the authenticity of the recipient of the document; and

releasing the document when the intended recipient has proved their identity by use of the first token of the intended recipient that is uniquely related to the second token of the intended recipient.

(Emphasis added).

Applicant respectfully submits that independent claim 1 is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further

view of *Menezes* does not disclose, teach, or suggest at least "receiving and securely retaining a digital document and a transmitted independently verifiable data record of the intended recipient at a printout station, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender" or "decoding encrypted identification data with the first token of the intended recipient, the encrypted identification data being identification data from the independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station," as emphasized above.

The Office Action of December 8, 2006 cites *Mazzagatte* in support of disclosing the features directed at verifying the identity of an intended recipient of a document. However, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node. Further, *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes. Thus, *Mazzagatte* fails to teach or show an "independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station," as recited in the claim. (Emphasis added).

Linsker is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linsker* does not teach or suggest that information is encrypted

using a token of an intended recipient and then transmitted. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linsker* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as an "independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station," as recited in the claim. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim

1. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 1 is not obvious under the proposed combination, and the rejection should be overturned.

Further, in the final Office Action issued May 24, 2007, the Examiner contends that "Menezes and Davis at the very least suggest encrypting identifying information with the public key of the intended recipient and transmitting that information from the sender." Page 3. In response, Applicant notes that *Davis* and *Menezes* disclose a type of authentication of executing a challenge/response protocol with a public token of an intended recipient. Neither *Davis* nor *Menezes* discloses using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient. On this point, the Examiner states that the *Menezes* and *Davis* combination "fairly suggests that such encryption would take place at the sender before the document as a whole would be sent (noting in particular the disclosure in Davis of the document and control information of the header being encrypted at the sender, column 4, line 39-column 5, line 9)." Final Office Action, page 4. In response, Applicant notes that this portion of the *Davis* disclosure refers to encryption using a public key of a printing node and not that of an intended recipient. Therefore, the proposed combination does not teach or suggest the aforementioned features.

For at least these reasons, the rejection should be overturned.

2. Claims 2-8

Dependent claims 2-8 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that the dependent claims 2-8 contain all features of allowable independent claim 1. *See, e.g., In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988). Accordingly, the rejection to these claims should be overturned.

3. Claim 9

As provided in independent claim 9, Applicant claims:

> A method of sending and delivering a digital document to an intended recipient at a printout station together with data enabling the document and the sender to be authenticated, the method comprising:
>
> creating a digest of the document using a hash algorithm;
>
> obtaining a first token of the intended recipient;
>
> encrypting the digest using a first token of the sender;
>
> obtaining a second token of the sender relating to the first token of the sender, which can be used to decrypt the encrypted digest;
>
> ***encoding identification data of the intended recipient using the first token of the intended recipient;***
>
> ***sending the encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient;***
>
> receiving and securely retaining a transmitted document, the encoded identification data, and a transmitted independently verifiable data record of the intended recipient at a printout station;
>
> requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient;
>
> decoding the identification data of the intended recipient using a second token of the intended recipient;
>
> comparing the decoded identification data with contents of the independently verifiable data record to determine the authenticity of the recipient of the document; and

releasing the document when the intended recipient has proved their identity by use of the second token of the intended recipient that is uniquely related to the first token of the intended recipient.

(Emphasis added).

Applicant respectfully submits that independent claim 9, as amended, is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* does not disclose, teach, or suggest at least "encoding identification data of the intended recipient using the first token of the intended recipient" and "sending the encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient," as emphasized above.

The Office Action of December 8, 2006 cites *Mazzagatte* in support of disclosing the features directed at verifying the identity of an intended recipient of a document. However, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node. Further, *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes. Thus, *Mazzagatte* fails to teach or show "encoding identification data of the intended recipient using the first token of the intended recipient" and "sending the

encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient," as recited in the claim.

Linsker is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linsker* does not teach or suggest that information is encrypted using a token of an intended recipient and then transmitted. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linsker* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient. Applicant respectfully submits that *Menezes* describes a challenge-response technique where a random number is encrypted and does not teach or suggest "encoding identification data of the intended recipient using the first token of the intended recipient," as recited in claim 9.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the

document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as "encoding identification data of the intended recipient using the first token of the intended recipient" and "sending the encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient," as recited in the claim. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 9. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 9 is not obvious under the proposed combination, and the rejection should be overturned.

4. Claims 10-12 and 14-17

Dependent claims 10-12 and 14-17 (which depend from independent claim 9) are allowable as a matter of law for at least the reason that the dependent claims 10-12 and 14-17 contain all features of allowable independent claim 9. Accordingly, the rejection to these claims should be withdrawn.

5. Claim 18

As provided in independent claim 18, Applicant claims:

A device for delivering and determining the authenticity of a digital document sent by an unknown sender to an intended recipient at a printout station, the device comprising:

a communications module arranged to receive an electronic version of the transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender, a second token relating to the first token of the sender, and encrypted identification data of the intended recipient, the encrypted identification data being encrypted using a first token of the intended recipient;

a store for securely retaining the transmitted document, the transmitted independently verifiable data record and the first token of the intended recipient;

an instruction module for requesting proof of the intended recipient's identity using data provided in the intended recipient's data record; and

a controller arranged to decode the encrypted digest using the second token of the sender; creating a digest of the document using a hash algorithm; comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document; and releasing the document when the intended recipient has proved their identity by use of a second token of the intended recipient that is uniquely related to the first token of the intended recipient, wherein the second token of the intended recipient is used to decode encrypted identification data of the intended recipient that is compared to contents of the independently verifiable data record of the intended recipient to determine authenticity of the intended recipient.

(Emphasis added).

Applicant respectfully submits that independent claim 18, as amended, is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* does not disclose, teach, or suggest at least "a communications module arranged to receive an electronic version of the

transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender, a second token relating to the first token of the sender, and encrypted identification data of the intended recipient, the encrypted identification data being encrypted using a first token of the intended recipient," as emphasized above.

Further, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node, and *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes. Thus, *Mazzagatte* fails to teach or show "a communications module arranged to receive an electronic version of the transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender, a second token relating to the first token of the sender, and encrypted identification data of the intended recipient, the encrypted identification data being encrypted using a first token of the intended recipient," as recited in the claim.

Linsker is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linsker* does not teach or suggest that information is encrypted using a token of an intended recipient and then transmitted. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linsker* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient.

Applicant respectfully submits that *Menezes* describes a challenge-response technique where a random number is encrypted and does not teach or suggest "wherein the second token of the intended recipient is used to decode encrypted identification data of the intended recipient that is compared to contents of the independently verifiable data record of the intended recipient to determine authenticity of the intended recipient," as recited in claim 18.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the

document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as "wherein the second token of the intended recipient is used to decode encrypted identification data of the intended recipient that is compared to contents of the independently verifiable data record of the intended recipient to determine authenticity of the intended recipient," as recited in the claim. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 18. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 18 is not obvious under the proposed combination, and the rejection should be overturned.

6. Claim 19

As provided in independent claim 19, Applicant claims:

> A device for sending and delivering a digital document to an intended recipient at a printout station together with data enabling the document and the sender to be authenticated, the device comprising:
> ***a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the sender and to encrypt identification data of the intended recipient using a first token of the intended recipient;*** and

a communications module arranged to obtain a second token of the sender related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document, the second token of the sender, the encrypted identification data of the intended recipient, and the first token of the intended recipient to the recipient.

(Emphasis added).

Applicant respectfully submits that independent claim 19, as amended, is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* does not disclose, teach, or suggest at least "a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the sender and to encrypt identification data of the intended recipient using a first token of the intended recipient" and "a communications module arranged to obtain a second token of the sender related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document, the second token of the sender, the encrypted identification data of the intended recipient, and the first token of the intended recipient to the recipient," as emphasized above.

Further, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node, and *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for

identification verification or authentication purposes. Thus, *Mazzagatte* fails to teach or show "a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the sender and to encrypt identification data of the intended recipient using a first token of the intended recipient" and "a communications module arranged to obtain a second token of the sender related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document, the second token of the sender, the encrypted identification data of the intended recipient, and the first token of the intended recipient to the recipient," as recited in the claim.

Linsker is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linsker* does not teach or suggest that information is encrypted using a token of an intended recipient and then sent to a recipient. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linsker* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient. Applicant respectfully submits that *Menezes* describes a challenge-response technique where a random number is encrypted and does not teach or suggest "to encrypt identification data of the intended recipient using a first token of the intended recipient," as recited in claim 19.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as "to encrypt identification data of the intended recipient using a first token of the intended recipient," as recited in the claim. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 19. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 19 is not obvious under the proposed combination, and the rejection should be overturned.

F. Applicant's Claim 13

Claim 13 was rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* in further view of *Clark* (U.S. Patent 5,448,045). Dependent claim 13 (which depends from independent claim 9) is allowable as a matter of law for at least the reason that the dependent claim 13 contains all features of allowable independent claim 9 and *Clark* does not remedy the deficiencies of the *Linsker*, *Mazzagatte*, and *Menezes* references. Accordingly, the rejection to this claim should be overturned.

VIII. Conclusion

In summary, it is Applicant's position that Applicant's claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: 

Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A method of delivering and determining the authenticity of a digital document sent by an unknown sender to an intended recipient at a printout station, the method comprising:

receiving and securely retaining a digital document and a transmitted independently verifiable data record of the intended recipient at a printout station, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender;

obtaining a second token of the sender relating to the first token of the sender;

obtaining a first token of the intended recipient;

decoding the encrypted digest using the second token of the sender;

using a hash algorithm to create a digest of the document;

comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document;

requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient;

decoding encrypted identification data with the first token of the intended recipient, the encrypted identification data being identification data from the

independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station;

comparing the decrypted identification data with contents of the independently verifiable data record to determine the authenticity of the recipient of the document; and

releasing the document when the intended recipient has proved their identity by use of the first token of the intended recipient that is uniquely related to the second token of the intended recipient.

2. A method according to Claim 1, wherein the receiving step comprises receiving a digital certificate of the sender.

3. A method according to Claim 2, wherein the obtaining a second token of the sender step comprises the second token of the sender being sent as part of the sender's digital certificate.

4. A method according to Claim 2, further comprising carrying out an on-line check of the validity of the sender's certificate.

5. A method according to Claim 1, wherein the first and second tokens of the sender comprise private and public encryption/decryption keys of the sender and the first and second tokens of the intended recipient comprise private and public encryption/decryption keys of the intended recipient.

6. A method according to Claim 1, further comprising printing out a copy of the document once the sender and the document have been authenticated.

7. A method according to Claim 6, wherein the method further comprises printing a verifying mark on the printed copy of the document to signify its authenticity.

8. A method according to Claim 1, wherein the transmitted document comprises a fax document.

9. A method of sending and delivering a digital document to an intended recipient at a printout station together with data enabling the document and the sender to be authenticated, the method comprising:

creating a digest of the document using a hash algorithm;

obtaining a first token of the intended recipient;

encrypting the digest using a first token of the sender;

obtaining a second token of the sender relating to the first token of the sender, which can be used to decrypt the encrypted digest;

encoding identification data of the intended recipient using the first token of the intended recipient;

sending the encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient;

receiving and securely retaining a transmitted document, the encoded identification data, and a transmitted independently verifiable data record of the intended recipient at a printout station;

requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient;

decoding the identification data of the intended recipient using a second token of the intended recipient;

comparing the decoded identification data with contents of the independently verifiable data record to determine the authenticity of the recipient of the document; and

releasing the document when the intended recipient has proved their identity by use of the second token of the intended recipient that is uniquely related to the first token of the intended recipient.

10. A method according to Claim 9, wherein the transmitted document is a fax document.

11. A method according to Claim 9, further comprising the sender proving their identity prior to the sending step by transferring data from a personal portable data carrier holding the first token of the sender to a transmission station from which the document is to be sent.

12. A method according to Claim 11, wherein the proving step further comprises the sender entering a verifiable security identifier into the transmission station to establish that they are the legitimate owner of the portable data carrier.

13. A method according to Claim 11, wherein the step of encrypting the digest comprises supplying the digest of the document from the transmission station to the portable data carrier of the sender, encrypting the digest of the document on the portable data carrier, and returning the encrypted digest of the document from the portable data carrier to the transmission station.

14. A method according to Claim 9, further comprising obtaining details of the sender including the second token of the sender prior to transmitting the document.

15. A method according to Claim 14, wherein the step of obtaining details comprises obtaining the sender's details from a central database storing second tokens of the senders and other sender's details.

16. A method according to Claim 14, wherein the sender's details and the second token of the sender are provided in a sender's digital certificate.

17. A method according to any of Claim 9, wherein the first and second tokens of the sender comprise private and public encryption/decryption keys of the sender.

18. A device for delivering and determining the authenticity of a digital document sent by an unknown sender to an intended recipient at a printout station, the device comprising:

a communications module arranged to receive an electronic version of the transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender, a second token relating to the first token of the sender, and encrypted identification data of the intended recipient, the encrypted identification data being encrypted using a first token of the intended recipient;

a store for securely retaining the transmitted document, the transmitted independently verifiable data record and the first token of the intended recipient;

an instruction module for requesting proof of the intended recipient's identity using data provided in the intended recipient's data record; and

a controller arranged to decode the encrypted digest using the second token of the sender; creating a digest of the document using a hash algorithm; comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document; and releasing the document when the intended recipient has proved their identity by use of a second token of the intended recipient that is uniquely related to the first token of the intended recipient, wherein the second token of the intended recipient is used

to decode encrypted identification data of the intended recipient that is compared to contents of the independently verifiable data record of the intended recipient to determine authenticity of the intended recipient.

19. A device for sending and delivering a digital document to an intended recipient at a printout station together with data enabling the document and the sender to be authenticated, the device comprising:

a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the sender and to encrypt identification data of the intended recipient using a first token of the intended recipient; and

a communications module arranged to obtain a second token of the sender related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document,

the second token of the sender, the encrypted identification data of the intended recipient, and the first token of the intended recipient to the recipient.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There have been no decisions rendered by a court or Board in related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.